Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Beniamino Segre

Ovali e curve a nei piani di Galois di caratteristica due

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **32** (1962), n.6, p. 785–790.

Accademia Nazionale dei Lincei

¡http://www.bdim.eu/item?id=RLINA_1962_8_32_6_785_0¿

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Accademia Nazionale dei Lincei, 1962.

RENDICONTI

DELLE SEDUTE

DELLA ACCADEMIA NAZIONALE DEI LINCEI

Classe di Scienze fisiche, matematiche e naturali

Seduta del 12 giugno 1962

Presiede il Presidente GINO CASSINIS

NOTE DI SOCI

Matematica. — *Ovali e curve σ nei piani di Galois di caratteristica due* (*). Nota del Socio BENIAMINO SEGRE.

La presente Nota espone brevemente alcuni risultati di geometria finita i quali, assieme ad altri, verranno stabiliti in un lavoro di prossima pubblicazione. In tale lavoro verrà pur data la bibliografia sull'argomento.

I. – DIAGRAMMI DI TRASLAZIONE.

Fissato un punto P improprio di uno spazio affine S, di dimensione $r+1 \geq 2$, chiameremo *diagramma* relativo a P un qualunque insieme Ω di punti il quale abbia uno ed un sol punto sopra ogni retta di S uscente da P. È chiaro che, introdotte in S coordinate $(x_1, x_2, \cdots, x_r, y)$ tali che P risulti il punto all'infinito dell'asse y, l'equazione di Ω è allora della forma

$$y = f(x_1, x_2, \cdots, x_r), \tag{1}$$

ove $f(x_1, x_2, \cdots, x_r)$ designa una funzione univoca delle x definita per valori arbitrari di questi argomenti; e viceversa.

(*) Presentata nella seduta del 12 giugno 1962.

Il diagramma Ω verrà detto di *traslazione* quand'esso sia trasformato in sé da ogni traslazione che muti l'uno nell'altro due punti di Ω comunque scelti; e questo si traduce in ciò che l'equazione funzionale

$$(2) \qquad f(x_1 + c_1, x_2 + c_2, \cdots, x_r + c_r) = f(x_1, x_2, \cdots, x_r) + \\ + f(c_1, c_2, \cdots, c_r) - f(0, 0, \cdots, 0)$$

debba sussistere identicamente nelle x, c. La (2) è manifestamente sempre soddisfatta da una qualsiasi funzione lineare delle x; corrispondentemente, la (1) fornisce gli iperpiani di S non passanti per P.

Nel caso in cui lo spazio affine S sia finito, e cioè risulti definito sopra un qualunque campo di Galois

$$(3) \qquad \gamma = \mathrm{GF}(q), \qquad \text{con} \quad q = p^t, \qquad p \text{ primo},$$

vale il seguente teorema, il quale fornisce dunque la completa soluzione della (1) in γ.

Sopra un qualsiasi campo γ, *dato dalla* (3), *i diagrammi di traslazione sono tutti e soli quelli rappresentabili con un'equazione della forma*

$$y = a_0 + \sum_{i=1}^{r} \sum_{j=0}^{t-1} a_{ij} x_i^{p^j},$$

ove le a designano elementi arbitrari di γ.

Si prova inoltre che:

In uno spazio $S_{r+1,q}$ (*proiettivo*) *di Galois, i soli insiemi di punti che porgano in duplice modo un diagramma di traslazione, relativamente ad uno stesso punto* P *ed a due diversi iperpiani per* P *quali iperpiani impropri, son dati dagli iperpiani e, se* $p = 2$, *dalle quadriche di* $S_{r+1,q}$ *specializzate* $r - 1$ *volte* (*di cui il nucleo, ma non – se* $r > 1$ – *il vertice, contenga* P).

II. – Il problema delle ovali.

Ricordiamo che chiamasi *k–arco* ogni insieme di k punti a tre a tre non allineati di un piano $S_{2,q}$ di Galois. Nello studio di tali insiemi, di recente ampiamente svolto e generalizzato agli spazi superiori da me e da altri, hanno particolare importanza le *ovali*, così chiamandosi i *k–archi* per i quali (corrispondentemente ad un dato $q = p^t$) k raggiunge il suo massimo.

Occorre distinguere al riguardo il caso in cui q è dispari (ossia $p > 2$) da quello in cui q è pari (ossia $p = 2$). Nel primo caso, le ovali sono i $(q + 1)$–archi, e questi – quali insiemi di punti – coincidono precisamente colle coniche di $S_{2,q}$.

Nel secondo caso ($q = 2^t$), si è tuttora ben lungi dal conoscere appieno la *struttura generale delle ovali* (e delle loro estensioni agli spazi superiori). Si sa soltanto ch'esse attualmente risultano $(q + 2)$–*archi*, esempi in proposito essendo dati dagli insiemi (di traslazione) definiti coll'aggregare ai punti di una conica (irriducibile) di $S_{2,q}$ il nucleo di questa. Mentre per $t = 1, 2, 3$ non vi sono altre ovali all'infuori di quegli insiemi, per tutti gli altri valori di t – ad eccezione di $t = 6$ – si conoscono esempi ulteriori (non ottenibili cioè in

tal guisa a partire da una conica), dati (per $t \neq 4, 6$) dagli insiemi che si hanno aggregando i punti all'infinito degli assi x, y a quelli di un diagramma di traslazione

$$y = x^{2^g} \qquad [\text{con } 2 \leq g \leq t-2, \quad (g,t) = 1].$$

Nel caso in questione ($q = 2^t$), il problema generale delle ovali si riconduce subito a vedere *quand'è che l'insieme ottenuto aggregando i punti all'infinito degli assi x, y ai punti del diagramma di equazione*

$$y = a_0 + a_1 x + a_2 x^2 + \cdots + a_{q-1} x^{q-1} \qquad (a_i \in \gamma) \tag{4}$$

risulta un'ovale. Una condizione manifestamente all'uopo necessaria, è che in γ la (4) definisca x quale funzione univoca della y; il che può tradursi nell'uguaglianza (identica rispetto a λ):

$$\{a_1, a_2, \cdots, a_{q-2}, a_{q-1} + \lambda\} = \lambda^{q-1} - 1, \tag{5}$$

dove il primo membro designa il determinante circolante una riga del quale è ivi indicata fra graffe.

Preso un qualunque punto al finito dell'insieme suddetto come origine O delle coordinate, ossia assunto in (4) $a_0 = 0$, la condizione affinché ogni retta per O incontri altrove l'insieme suddetto in uno ed un sol punto si traduce similmente nella

$$\{a_1 + \lambda, a_2, \cdots, a_{q-1}\} = \lambda^{q-1} - 1. \tag{6}$$

E si constata per esempio che, se $q = 8$, le (5), (6) sono sufficienti affinché la (4) definisca un'ovale.

Qualunque sia q, dalla (6) si traggono le condizioni necessarie:

$$a_1 = a_3 = a_5 = \cdots = a_{q-1} = 0 \tag{7}$$

[equivalenti a ciò che, nel secondo membro della (4), non abbiano a comparire che potenze pari della x]. Ma non pare agevole di trovare seguendo questa via condizioni necessarie e sufficienti.

Si raggiunge invece lo scopo introducendo (per ogni $k \geq 0$) i polinomi omogenei

$$\sigma_k(x, x_1, x_2) = \sum_{i+i_1+i_2=k} x^i x_1^{i_1} x_2^{i_2}, \tag{8}$$

i quali possono anche venir scritti nella forma:

$$\sigma_k(x, x_1, x_2) = \sum_{h=0}^{k} x^h \rho_{k-h}(x_1, x_2), \tag{8'}$$

avendo posto $\rho_0 = 1$ e (per ogni $k > 0$)

$$\rho_k(x_1, x_2) = x_1^k + x_1^{k-1} x_2 + \cdots + x_2^k = (x_1^{k+1} - x_2^{k+1})/(x_1 - x_2). \tag{9}$$

Invero, assunto in relazione alla (4)

$$\tau(x, x_1, x_2) = \sum_{k=2}^{q-1} a_k \sigma_{k-2}(x, x_1, x_2),$$

si constata facilmente come le condizioni richieste possano ricondursi a ciò che:

Nello spazio affine sopra γ *ove le* (x, x_1, x_2) *sono coordinate di punto, la superficie di equazione* $\tau(x, x_1, x_2) = 0$ *non deve contenere nessun punto che non stia su almeno uno dei piani* $x = x_1$, $x = x_2$, $x_1 = x_2$.

Nel caso più semplice in cui la (4) si riduca alla

$$y = x^{k+2}, \tag{10}$$

k deve intanto essere p a r i in virtù delle (7); deve inoltre valere la

$$(k + 2, q - 1) = 1, \tag{11}$$

traducente l'univoca risolubilità della (10) rispetto ad x. Allora la condizione necessaria e sufficiente data dall'ultimo enunciato può venire semplificata col dire che:

Nel piano di Galois sopra γ *ove le* (x, x_1, x_2) *son coordinate proiettive omogenee di punto, la curva (d'ordine* k*)* σ_k, *di equazione* $\sigma_k(x, x_1, x_2) = 0$, *non deve contenere nessun punto su* γ *ad eccezione al più del punto unità* U $(1, 1, 1)$.

Si può inoltre stabilire che:

Non appena q *(e quindi* t*) sia abbastanza grande rispetto a* k, *affinché* σ_k *soddisfi alla condizione specificata nell'ultimo enunciato occorre (ma generalmente non basta) che la curva* σ_k *risulti assolutamente r i d u c i b i l e (e cioè abbia a spezzarsi in un'opportuna estensione di* γ).

Siffatta r i d u c i b i l i t à ha ad esempio luogo se k è della forma

$$k = 2^s - 2,$$

sussistendo allora l ' i d e n t i t à

$$\sigma_k(x, x_1, x_2) = \rho_k(x + x_1, x + x_2); \tag{12}$$

corrispondentemente, si giunge così per nuova via alle *ovali di traslazione* dianzi segnalate.

Un altro caso di r i d u c i b i l i t à si ha per $k = 4$ a norma dell'identità

$$\sigma_4(x, x_1, x_2) = \{\sigma_2(x, x_1, x_2) + \varepsilon[\sigma_1(x, x_1, x_2)]^2\}\{\sigma_2(x, x_1, x_2) + \varepsilon^2[\sigma_1(x, x_1, x_2)]^2\},$$

facilmente dimostrabile, nella quale ε designa una radice dell'equazione

$$\varepsilon^2 + \varepsilon + 1 = 0. \tag{13}$$

Tale identità mostra che la curva σ_4 non ha punti in γ se, e soltanto se, la (13) non ammette radici in γ; e questo equivale a ciò che t sia d i s p a r i. Se ne trae che:

Per ogni $q = 2^t$ *con* t *dispari, aggregando i punti all'infinito degli assi* x, y *a quelli della curva* $y = x^6$ *si ottiene un'ovale, la quale risulta di traslazione soltanto nei casi* $t = 1$ *e* $t = 3$.

III. – Singolarità e riducibilità di polinomi ρ e di curve σ.

Gli sviluppi suaccennati suggeriscono parecchi interrogativi, a taluno dei quali daremo ora risposta. I risultati conseguiti, anche se non hanno riflessi positivi immediati sul problema delle ovali, presentano interesse in sé da vari punti di vista.

Le forme ternarie $\sigma_k = \sigma_k(x, x_1, x_2)$, definite dalla (8) [od (8')], soddisfanno anzitutto alle identità:

$$(14) \qquad \begin{cases} \sigma_{2n} = \sigma_n^2 + (xx_1 + xx_2 + x_1 x_2)\,\sigma_{n-1}^2, \\ \sigma_{2n+1} = \sigma_1 \sigma_n^2 + xx_1 x_2 \sigma_{n-1}^2. \end{cases}$$

Le suddette σ si esprimono inoltre con le forme binarie ρ, definite dalla (9), mediante l'identità:

$$(15) \qquad \sigma_k(x, x_1, x_2) = \sum_{(h)_k} x^{k-h} \rho_h(x + x_1, x + x_2)$$

[generalizzante la (12) e da non confondersi con la (8')], dove la somma a secondo membro va estesa ai valori di h che si ottengono da k nel modo seguente. Si consideri l'espressione di $k+2$ nella numerazione a base 2: allora $h+2$ assume tutti e soli i valori che da tale espressione si ricavano col sostituirvi qualche cifra 1 (eventualmente nessuna, ma non tutte) con uno zero.

Ne consegue che la curva σ_k contiene il punto U se, e soltanto se,

$$k \equiv 2 \pmod 4$$

oppure

$$k \equiv 3 \pmod 4,$$

avendo allora in U la molteplicità m e le tangenti

$$\rho_m(x + x_1, x + x_2) = 0,$$

dove m si determina coll'osservare dapprima che nei due casi rispettivamente il numero $k+2$ o $k+1$ è divisibile per 4: detta 2^l la massima potenza del 2 che divide quel numero (onde $l \geq 2$), risulta precisamente $m = 2^l - 2$.

È ben noto che, affinché la forma binaria ρ_k – data dalla (9) – sia irriducibile sull'anello degli interi, occorre e basta che il numero $k+1$ sia primo. Designando ancora per il momento con γ un campo finito (3) d'ordine q e caratteristica p qualsiansi (con $q = p^t$), si dimostra che:

Condizione necessaria e sufficiente affinché la forma binaria ρ_k *(di grado* $k \geq 2$*) sia irriducibile in* γ *è che valgano le*

$$(16) \qquad (k+1, p) = 1,$$

$$(17) \qquad (k+1, q^i - 1) = 1 \qquad \textit{per } i = 1, 2, \cdots, [\sqrt{k}\,].$$

Ove queste relazioni siano soddisfatte, la (17) *sussiste di conseguenza anche per* $i = [\sqrt{k}\,]+1, \cdots, k-1$, *ma non per* $i = k$, *ed inoltre* $k+1$ *risulta primo.*

Ritornando d'ora in poi al caso in cui $p = 2$ e poggiando sulla (15), dall'ultimo enunciato si trae agevolmente il seguente criterio d'irriducibilità.

Nell'ipotesi che k *sia della forma* $k = 8n + 2$, *con* $n \geq 1$, *e che valgano le* (17), *la curva* σ_k *risulta assolutamente irriducibile.*

È interessante rilevare come nel precedente enunciato le condizioni (17) possano venire omesse del tutto, ricorrendo a procedimenti d'altro tipo.

Così, ad esempio, si stabilisce l'*irriducibilità incondizionata* di σ_{10}, attraverso ad uno studio delle singolarità di questa curva. Dette singolarità consistono precisamente dei nove punti

$$U(1,1,1), \quad U_1(1,\varepsilon,\varepsilon^2), \quad U_2(1,\varepsilon^2,\varepsilon),$$
$$V_1(\varepsilon,1,1), \quad V_2(1,\varepsilon,1), \quad V_3(1,1,\varepsilon),$$
$$W_1(\varepsilon^2,1,1), \quad W_2(1,\varepsilon^2,1), \quad W_3(1,1,\varepsilon^2)$$

[dove ε denota una radice della (13)], i quali son tali che ciascuna delle rette congiungenti due punti scritti in righe diverse contiene un punto della riga rimanente. Poiché, a norma delle (14), σ_{10} ammette U_1, U_2 quali punti 4–pli, avendo in ognuno di essi un'unica tangente, data dalla $\sigma_1 = U_1U_2$ che ha incontro 5–punto con σ_{10} tanto in U_1 che in U_2, così un eventuale spezzamento di σ_{10} potrebbe soltanto aver luogo in due quintiche passanti l'una per U_1, ma non per U_2, e l'altra per U_2, ma non per U_1, contenenti ognuna ciascuno dei punti V e W; ora ciò è impossibile, in base agli allineamenti dei punti suddetti, onde l'asserto.

Un'analisi assai più complessa permette di stabilire l'annunciata *irriducibilità assoluta* di σ_{8n+2} per ogni $n \geq 1$ [mentre σ_2 si spezza in due rette uscenti da U, come si vede applicando la (12) per $g = k = 2$]. L'analisi si semplifica nel caso particolare in cui n sia una potenza del 2 ad esponente d i s p a r i (in quanto allora – in base alla (15) – $\sigma_k = \sigma_{8n+2}$ passa doppiamente per U, avendo ivi le tangenti distinte UU_1, UU_2, ciascuna delle quali ha con essa in U incontro k–punto), avendo riguardo al fatto generale che:

Una curva piana algebrica d'ordine $k \geq 2$, *definita sopra un campo qualsiasi, risulta necessariamente irriducibile nell'ipotesi ch'essa:* 1° *abbia in suo punto* U *incontro di molteplicità* k *con una retta la quale conti una volta sola fra le tangenti in* U, *e* 2° *non contenga come componente nessuna retta per* U.

Altri c r i t e r i d ' i r r i d u c i b i l i t à si stabiliscono in parte utilizzando ancora quest'ultima osservazione. Così, ad esempio, si prova che:

Se k *è della forma*

$$k = 2^a + 2^b - 2 \qquad (con\ 1 < a < b),$$

σ_k *risulta assolutamente irriducibile qualora sia* $(a, b) > 1$ *oppure, se* $(a, b) = 1$, *si supponga* $b \geq a + 2$ *e* $\rho_k(x_1, x_2)$ *irriducibile in* γ [per il che occorre e basta che valgano le (17)].

Si dimostra infine che *la curva* σ_{4n} *risulta assolutamente irriducibile per ogni* $n \geq 2$ (ma non, come s'è visto, per $n = 1$). Ciò si ottiene rilevando che l e s o l e singolarità di σ_{4n} son date dai $2n(2n-1)$ punti d i s t i n t i comuni alle curve σ_{2n} e σ_{2n-1} (mentre invece, se h è dispari, σ_h e σ_{h-1} non si incontrano in punti distinti); e che in ognuno di detti punti σ_{4n} ha precisamente una c u s p i d e o r d i n a r i a, ad esclusione soltanto di quelli fra essi che eventualmente giacciono sulla conica $xx_1 + xx_2 + x_1x_2 = 0$, e quindi pure – a norma della prima delle (14) – sulla curva σ_n, in ciascuno dei quali σ_{4n} ammette un t a c n o d o o r d i n a r i o.